



# **NMCI Server Transition Efforts, Supporting Architectures and Program of Record Information for Creating Compliant Applications**

Jeffery Naus  
NMCI Chief Engineer  
SPAWAR 055, PMW 164  
jeff.naus@navy.mil  
20 June 05

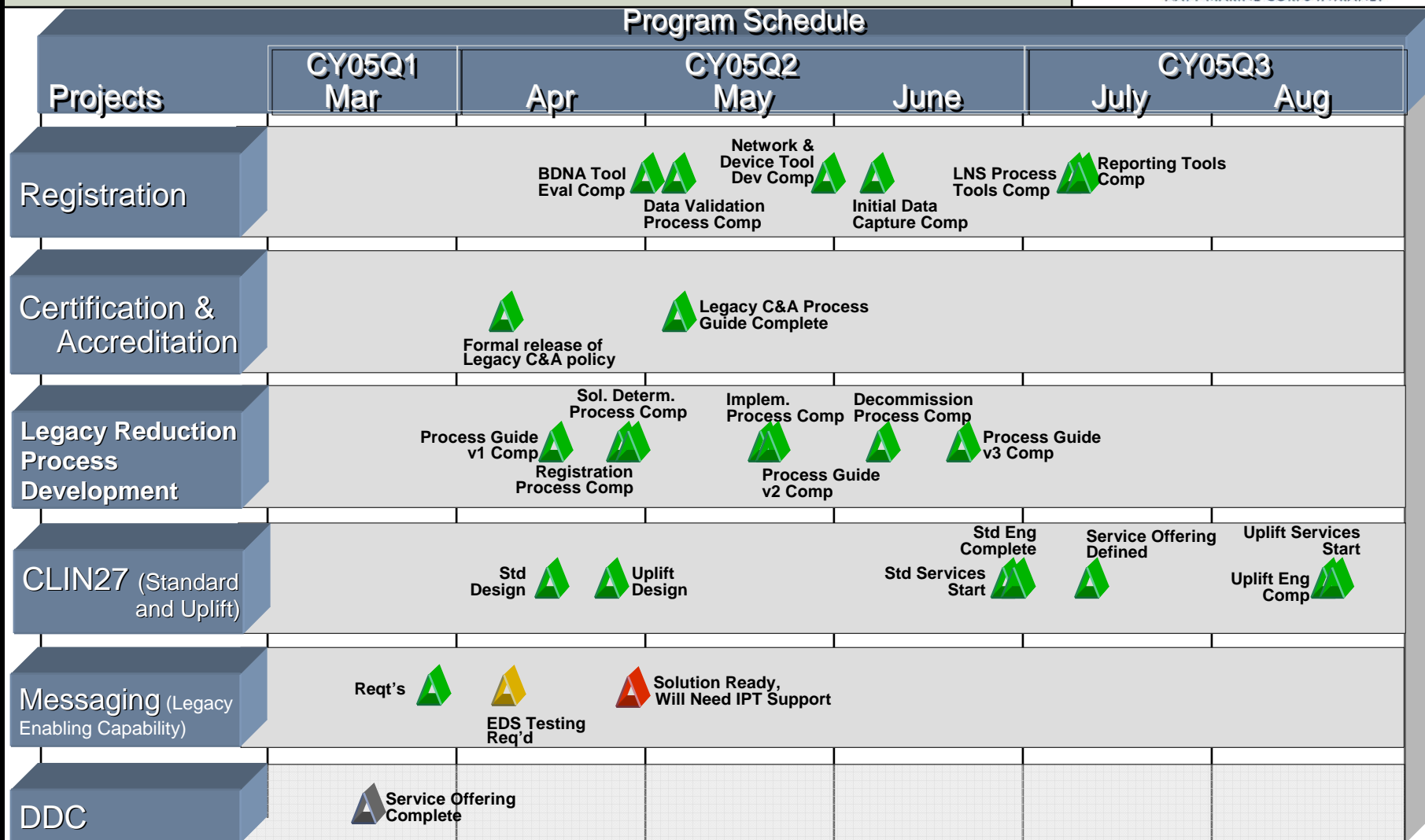
- **Seat cutover – complete by mid-2006**
- **Tech Refresh – XP SP2 & Office 2003 if site ready, otherwise Win 2K & Office 2003 on new HW**
- **Legacy Reduction** – driven by the FAM Process and need to eliminate the legacy networks
- **Customer Satisfaction – have to get better!**

***Legacy Network Reduction is one of  
ACNO-IT & DRPM priority areas***

- **Develop overall enterprise strategy to shut down legacy networks**
- **Determine solutions and policies required to successfully transition off legacy networks**
- **Develop a map of solutions and categories of applications**
- **Ensure that solutions are executable from the following perspectives:**
  - ☐ Business
  - ☐ Application
  - ☐ Technology
  - ☐ Organizational
  - ☐ Governance
- **Develop repeatable processes for the elimination of legacy networks**

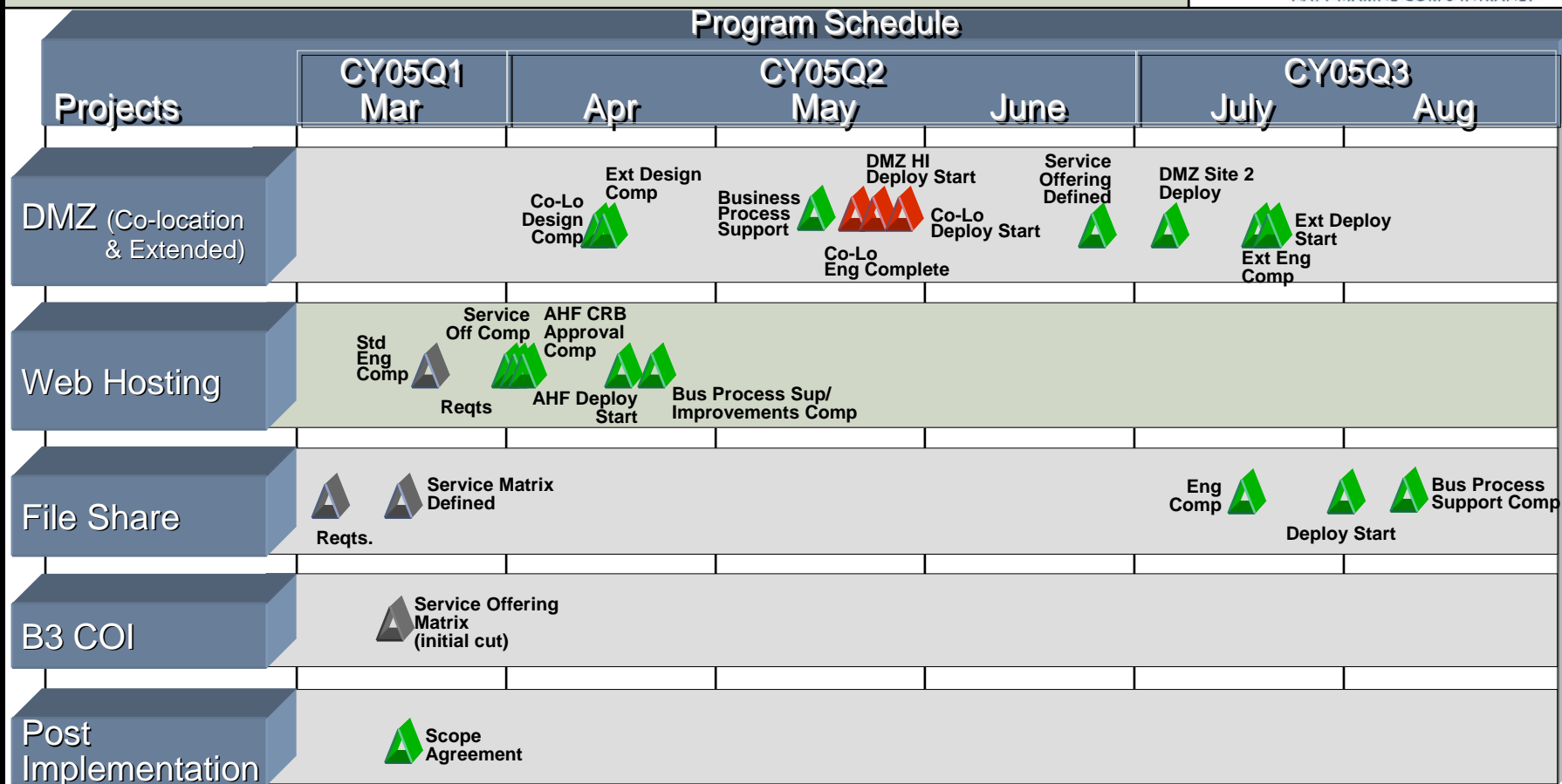
**The NMCI Information System Transition Team's (NISTT) efforts are a crucial component to make legacy network shutdown happen!**

# Key Milestones



 Complete
  High Risk For Meeting
  Moderate Risk For Meeting
  On track

# Key Milestones (Continued)



- **DMZ Schedule**
- **Coordination with ACNO(IT)**
- **Resolution of outstanding Web Hosting Issue**
- **BDNA Scanning**
- **Resolution of contracts issues with connecting Program of Record (POR) seats**
- **CLIN 27 Tactical Schedule**
  - ❑ We need to keep a “scorecard” for how many servers we transition off legacy networks
- **Formal Release of Legacy System Certification and Accreditation (C&A) Policy**
- **Overall program site legacy network shutdown schedule**



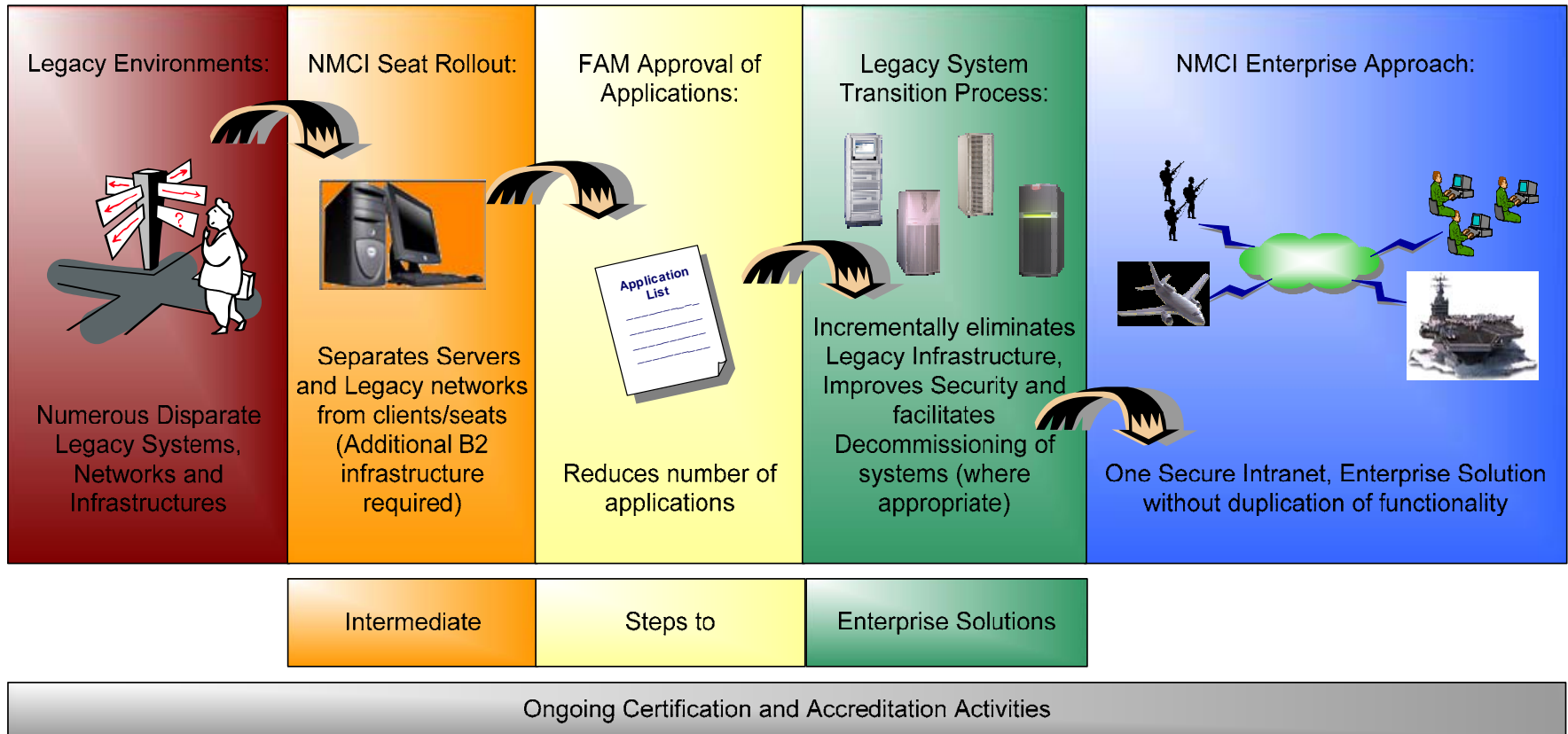
**\*The Five Dysfunctions of a Team**

**\*Source: "Overcoming The Five Dysfunctions of a Team"**  
**By Patrick Lencioni**


- **Develop overall enterprise strategy to shut down legacy networks**
- **Determine solutions and policies required to successfully transition off legacy networks**
- **Develop a map of solutions and categories of applications**
- **Ensure that solutions are executable from the following perspectives:**
  - ☐ Business
  - ☐ Application
  - ☐ Technology
  - ☐ Organizational
  - ☐ Governance
- **Develop repeatable processes for the elimination of legacy networks**



# Path to NMCI...an Enterprise Solution



# Network Roadmap

	NETWORKS	SERVERS	APPLICATIONS
<b>As - Is</b>	~ 850	~ 30K	<b>9352</b> (Approved/AWR)
<b>First Step</b>	20 % Reduction in Networks/Servers/Applications by OCT05		
<b>Goal</b>	NMCI/ISNS/ONENET/Other*  Minimum essential domain networks	(As Required)	(As Required)

## Business Value Metrics

ROI



Business Process Savings • Harvested Capabilities  
IT Infrastructure Savings • Hardware/Software/Admin.  
Infrastructure Savings • Electrical Power / Real-estate

Improved  
Security

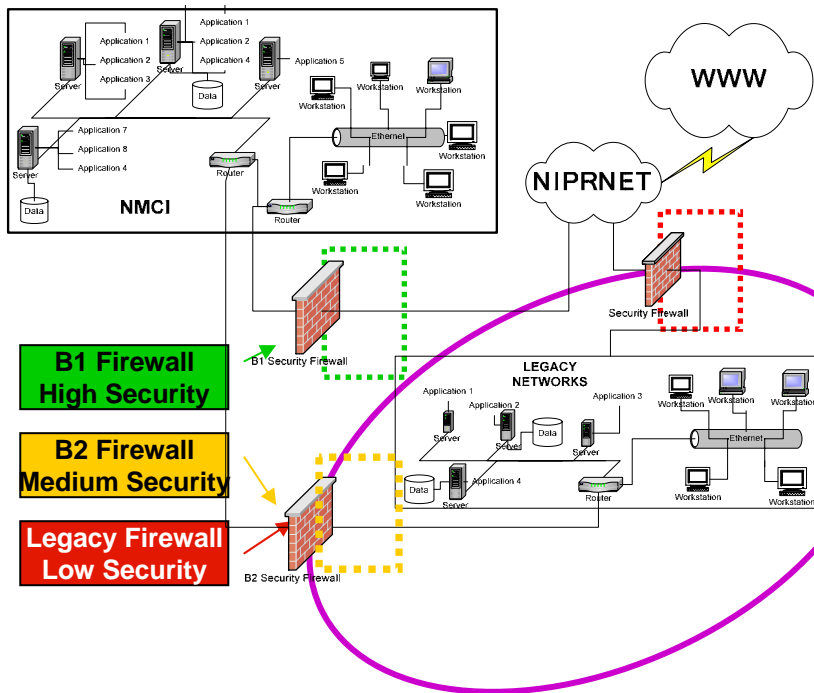


Information Security • Network Reliability/Availability

\* Potential Candidates: Virtual SYSCOMs RDT&E, S&T, BUMED, EDU Networks

# Challenges: Visibility, Technical Complexity & Quantity

- Multiple Interconnected Networks
- Owned by Separate Organizations
- Networks Connect Many:
  - Servers to Servers
  - Servers to Data Stores
  - Applications to Users
- Multiple Servers on Multiple Networks deliver same application to many users
- Lack of Inventory Control



**X ~ 850 = Complex Problem & Significant Security Implications**

# Legacy Network Shutdown Strategy



## Tactical Focus

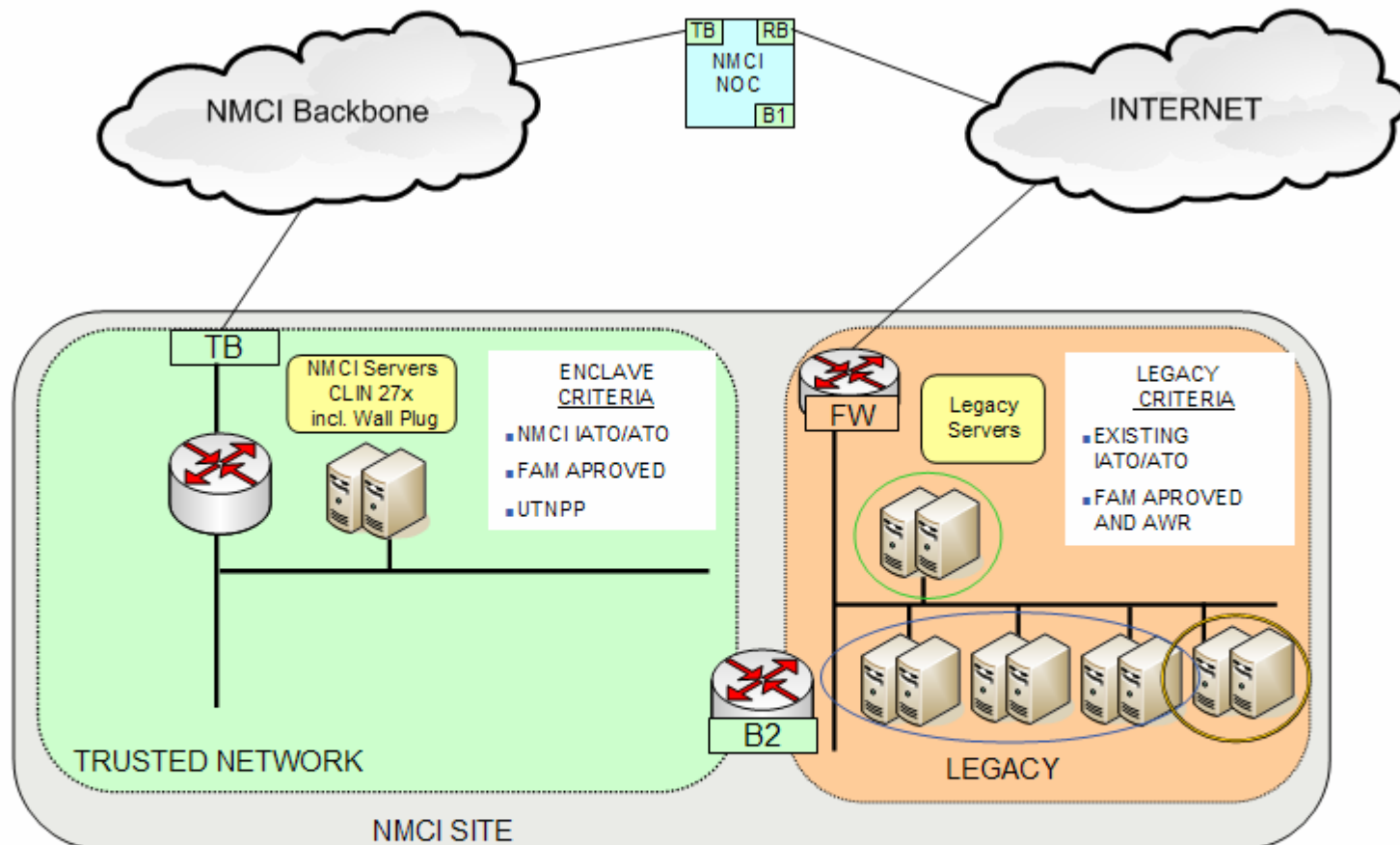
- ☐ Goal: Transition a minimum of 700 Legacy servers to NMCI by 30 September 05
- ☐ Identify and eliminate process bottlenecks within existing processes (e.g. C&A, ECCB)
- ☐ Adjust Technical Infrastructure support processes to ensure continuity of operations
- ☐ Identify servers/apps that can migrate using existing services on contract
  - Pre-Analysis by NISTT for technical and tactical compliance
- ☐ Submit and fulfill orders against existing services
- ☐ Expand contract to offer additional technical solutions
- ☐ Develop draft shutdown methodology; pilot with OBAN/SOBAN network
- ☐ Evaluate bDNA tool capability for use in discovery or registration processes

## Strategic Focus

- ☐ Goal: Transition all legacy networks to NMCI by 30 December 06
- ☐ Finalize and document shutdown methodology and processes, including solution determination business rules
- ☐ Develop processes and tools for enterprise planning and reporting
- ☐ Launch NMCI-wide Legacy Network Shutdown project at 21 June 2005 NMCI Enterprise Conference
  - Require formal reduction projects within each claimant

**Cyber Condition Zebra**

# NMCI – Current State



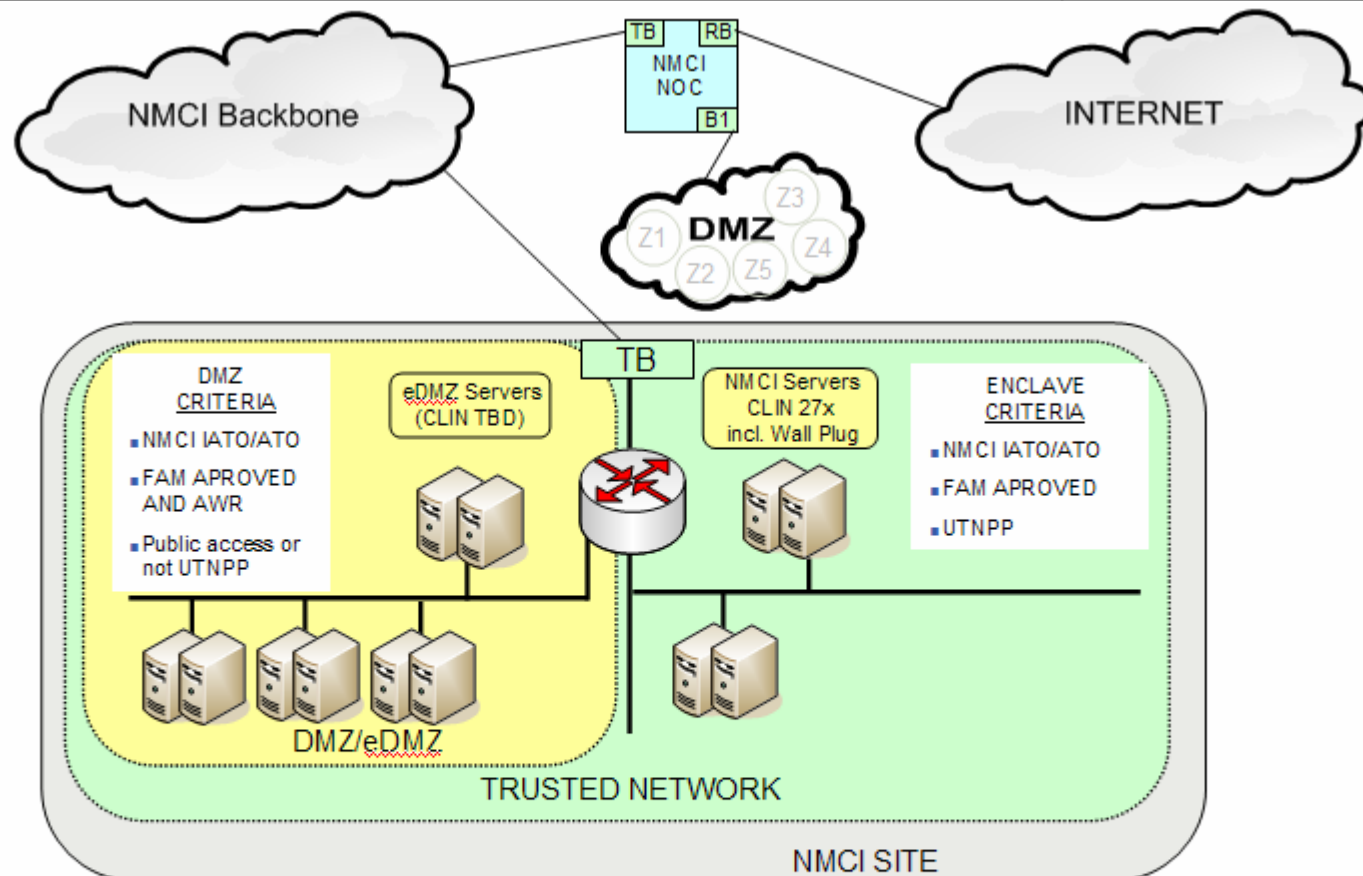
Few servers fully NMCI compliant, therefore, most servers remain on legacy network  
 Legacy environment has direct connection to internet and significant IA concerns  
 Est. 20% legacy servers are FAM approved and UTNPP compliant  
 Est. 10% legacy servers are FAM approved or FAM AWR and not UTNPP compliant or require public access  
 Est. 70% legacy servers are FAM AWR and UTNPP compliant

FAM approved fully  
UTNPP compliant

FAM AWR fully  
UTNPP compliant

FAM approved or  
AWR not UTNPP

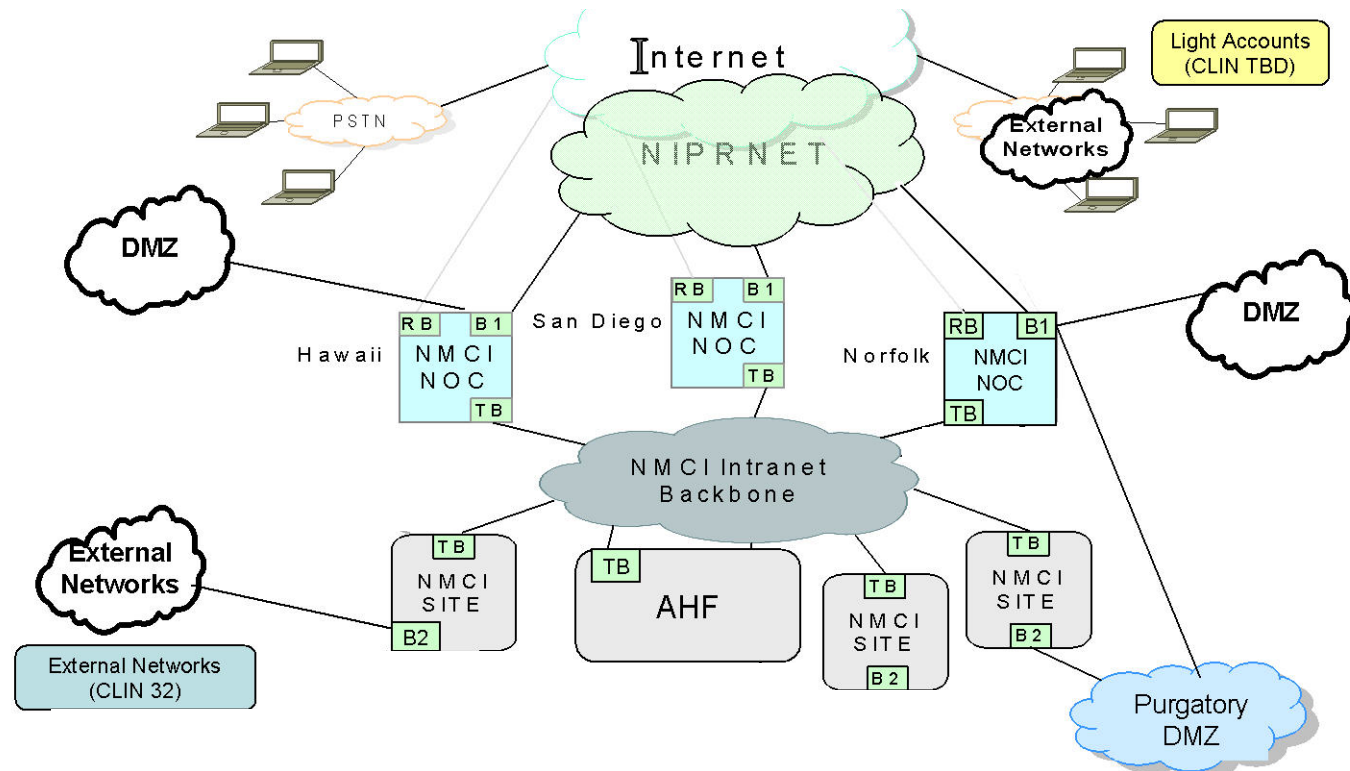
# NMCI – End State



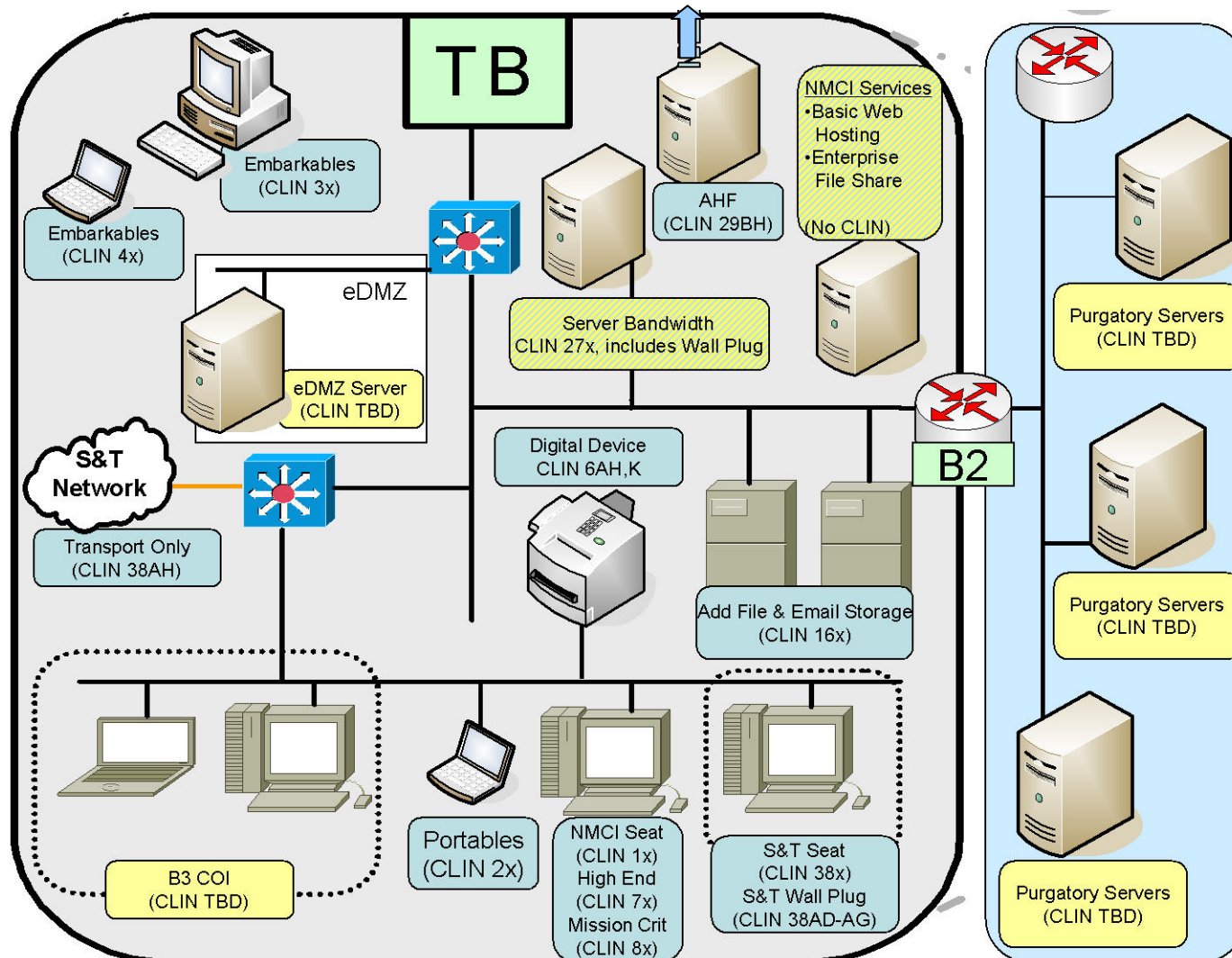
End state is elimination of legacy environment and all systems reside in NMCI



# EDS CLIN Diagram - Network



# EDS CLIN Diagram - Site





# CLIN 27 (Server Connections) Service Description



- CLIN 27 has 3 ordering options with 3 bandwidth configurations:
  - CLIN 0027 Standard: AA - Low, AB - Medium, AC – High
  - CLIN 0027 Mission Critical: AD - Low, AE - Medium, AF – High
  - CLIN 0027 Basic Service: AG - 5,000 servers or 2,100 applications at \$0.
- Wall plugs will be installed at sites with existing NMCI infrastructure
- CLIN 27 services categorized as Standard or Uplift.
- Standard Services available through the existing CLIN 27's and Uplifts through to-be-defined CLIN 27 options

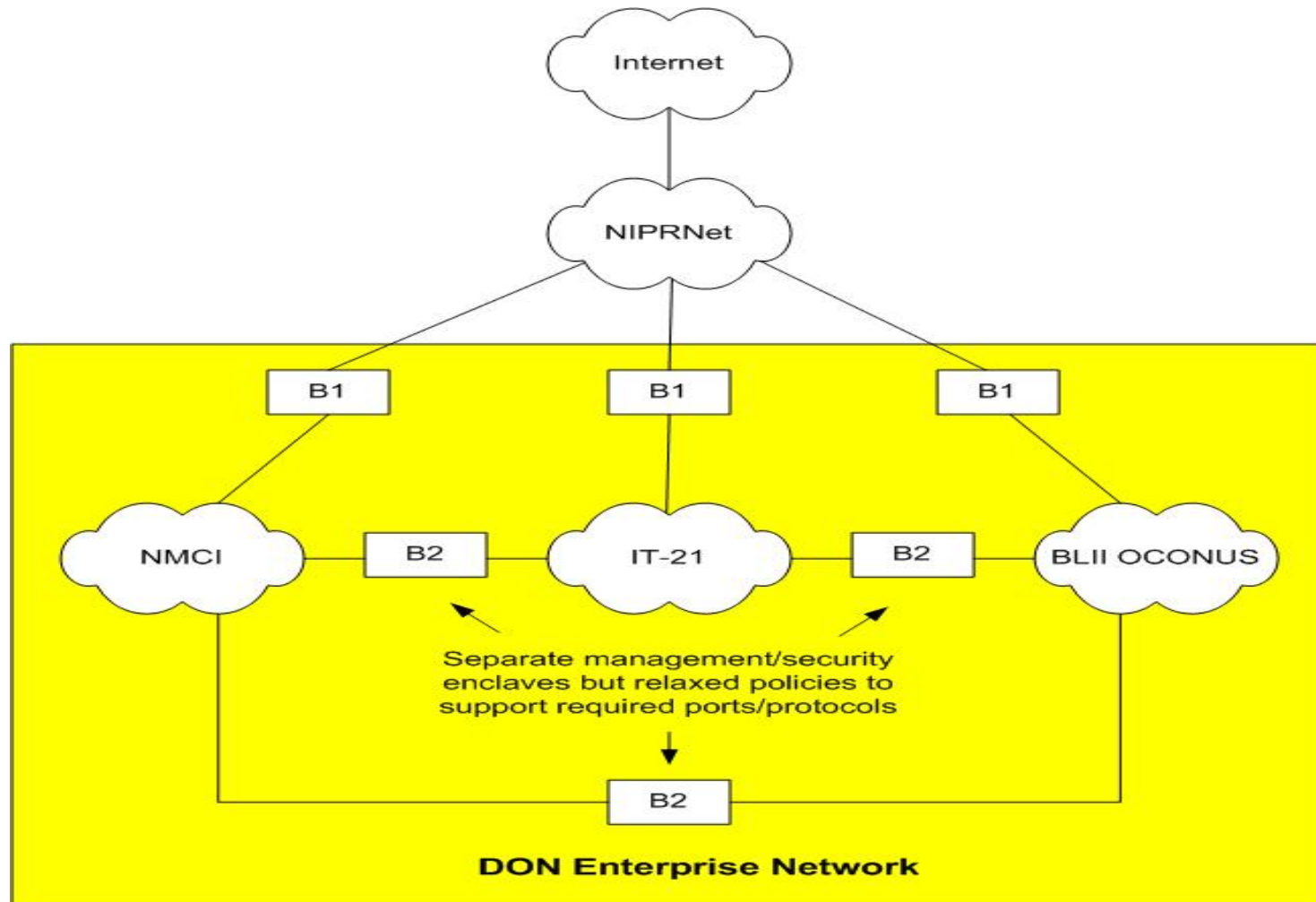
## Standard

- NMCI server name
- Static Internet Protocol (IP) addresses
- Public IP addresses
- Domain Name Servers (DNS)
- Connection Rates
- Help Desk Notification – Connection Status
- Failover Connection
- One-Way Trust to NMCI
- Active Directory Services
- Active Directory ID's for non-NMCI users (Bandwidth)
- Network Time Protocol (NTP)
- Remote Management, SMTP, Telnet, FTP, SSH
- SSL
- Authentication – Public Key Infrastructure (PKI)
- Multicasting
- Print Services – NMCI Printers
- Virus Scans / Updates

## Uplifts

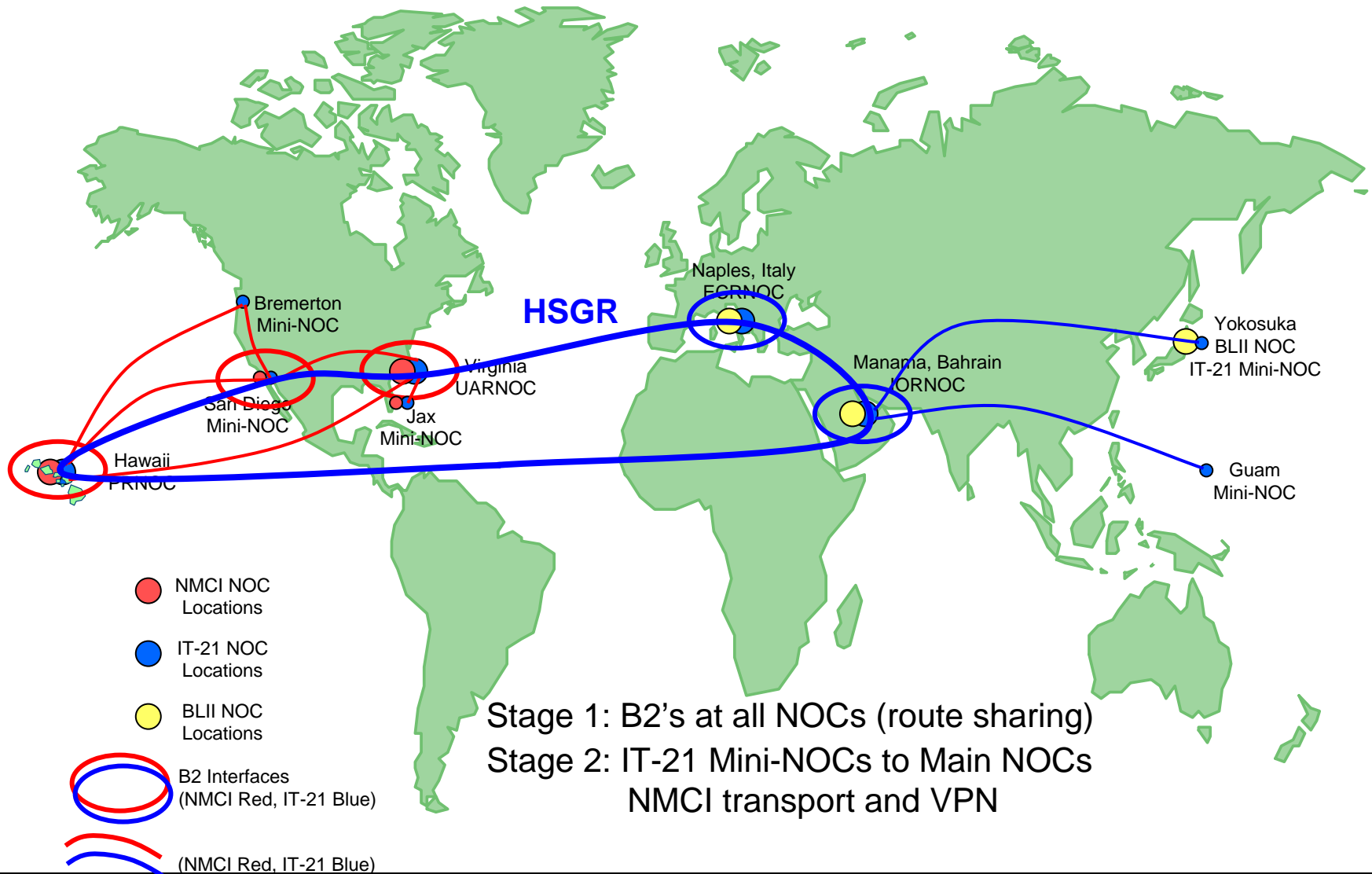
- Additional static IP addresses
- Additional public IP addresses
- DNS resolution to legacy environment
- WINS
- One-Way trust configuration
- LDAP Services
- Additional Remote management/File Transfer—SMTP, Telnet, FTP, SSH capabilities
- Installation and configuration of OCSP client
- Multicasting beyond standard service level
- Virus scans / Updates services
- Information Assurance Vulnerability Alert (IAVA) / Information Assurance Vulnerability Bulletins (IAVB) management

# Long Term: Navy Envisioned Connectivity

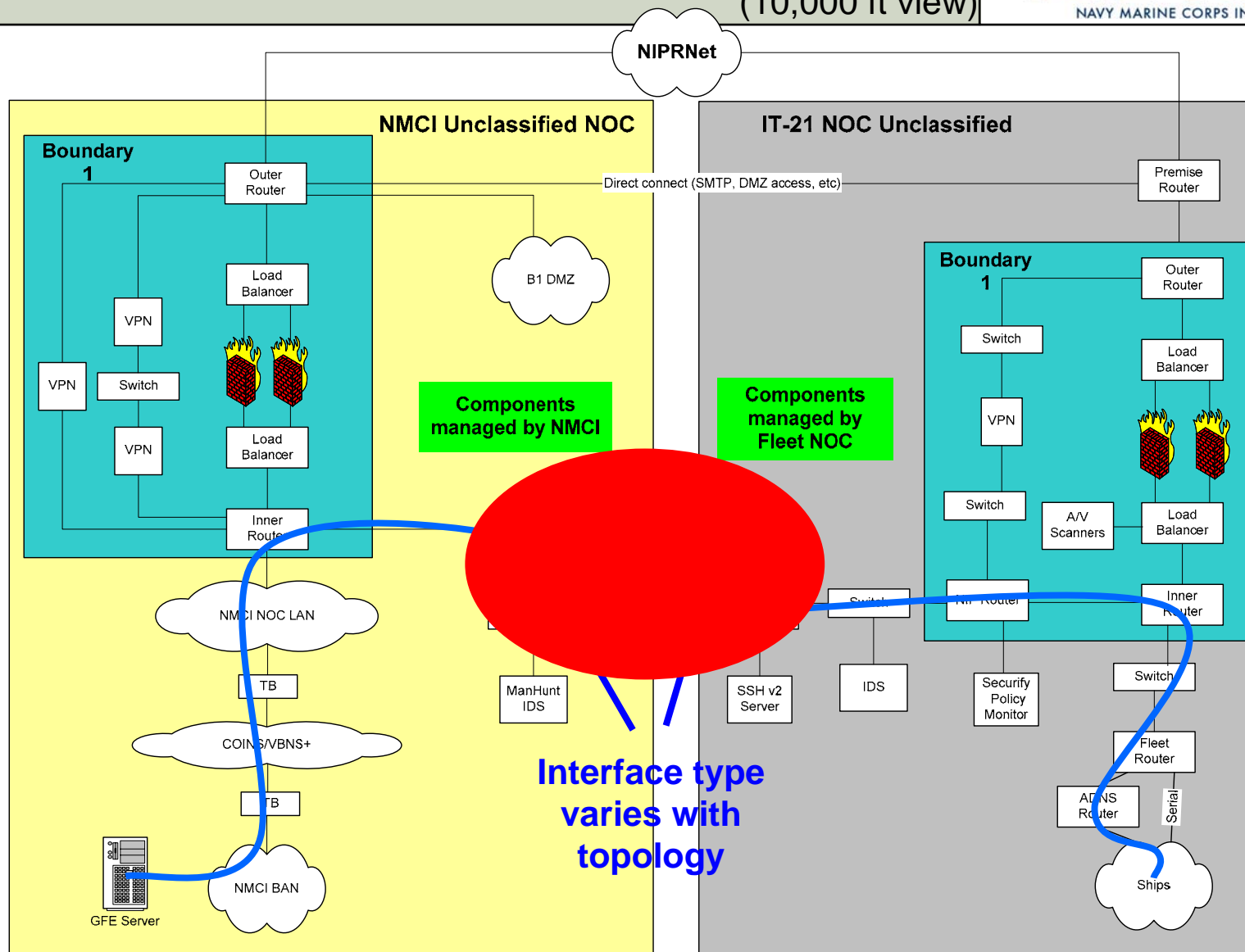


# How will it notionally work?

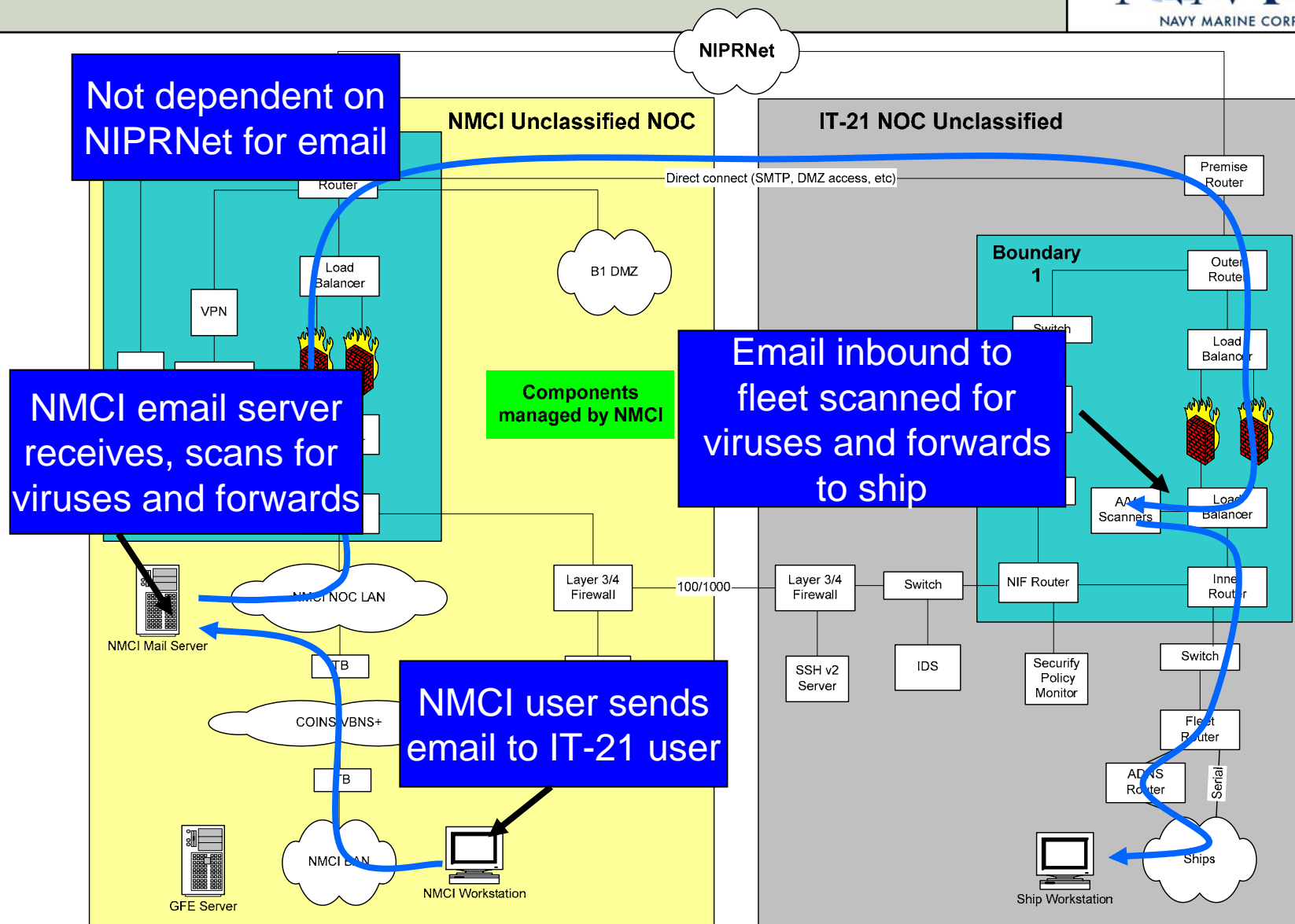
(100 mile high view)



# Notional B2 Interface NMCI-to-IT21 (10,000 ft view)



# Email Flow



➤ **Provide and extend system services for the DMZ.**

❑ These services include:

- Directory services
- Naming services
- Certificate revocation checking
- Web hosting
- Content management
- Authentication Services

➤ **Solution will employ many of the standard NMCI Network, IA and Help Desk structures and processes.**

➤ **The Design will meet the following goals established by NETWARCOM:**

- ❑ **DYNAMIC**, able to implement changing policies within a reasonably short period of time, whether planned or urgent.
- ❑ **AGILE**, able to support prompt migration of servers in and out of various zones during transition from legacy to fully NMCI or NMCI/DoD compliance.
- ❑ **ROBUST**, able to support a large number of servers both at remote Navy sites and at NMCI NOC facilities.
- ❑ **SECURE**, able to control and restrict access to specific resources while monitoring compliance with those controls.

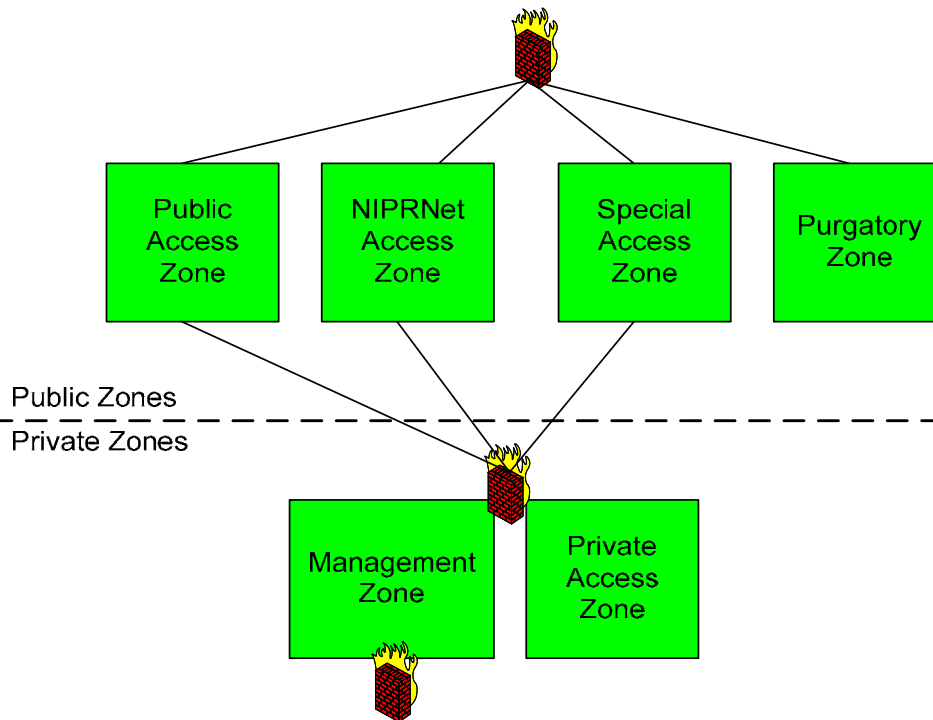
- **Primary function of the NMCI DMZ will be to protect resources requiring access from un-trusted environments**
- **The DMZ will include the ability for infrastructure services to be extended from the NMCI NOCs**
- **NMCI will host, manage and maintain responsibility for NMCI DMZ infrastructure servers**
- **The vast majority of the hosted systems will be operated by the Government who will retain responsibility for host and application security**
- **The DMZ Active Directory service will support:**
  - ☐ Authentication
  - ☐ Directory services – including some security group authorization
  - ☐ Network time
  - ☐ Windows Internet Naming Service (WINS)
  - ☐ Certificate revocation checking
  - ☐ Lightweight Directory Access Protocol (LDAP) queries

- **AHF deployed to host Customer applications on NMCI hardware**
- **DMZ deployment to support hosting of legacy servers**
- **AHF designed with zones in serial construct each separated by a firewall:**
  - ☐ Two Public Zones (Zones 0 & 1)
  - ☐ Two Private Zones (Zones 2 & 3)
  - ☐ One Management Zone (Zone 4)
  - ☐ One Backup Zone (Zone 5)
- **uB1 will utilize 4 public zones in parallel and two private zones all separated by firewall policies:**
  - ☐ Public Zones
    - Internet, NIPRNet, and Special Access Zones  
These zones may have connections to the Private Access Zones
    - Purgatory Zone  
No access to Private Access Zones
  - ☐ Private Zones (No NIPRNet/Internet connectivity)
    - Management Zone – Houses NMCI Infrastructure services
    - Private Access Zone – Will house Customer Application Servers.

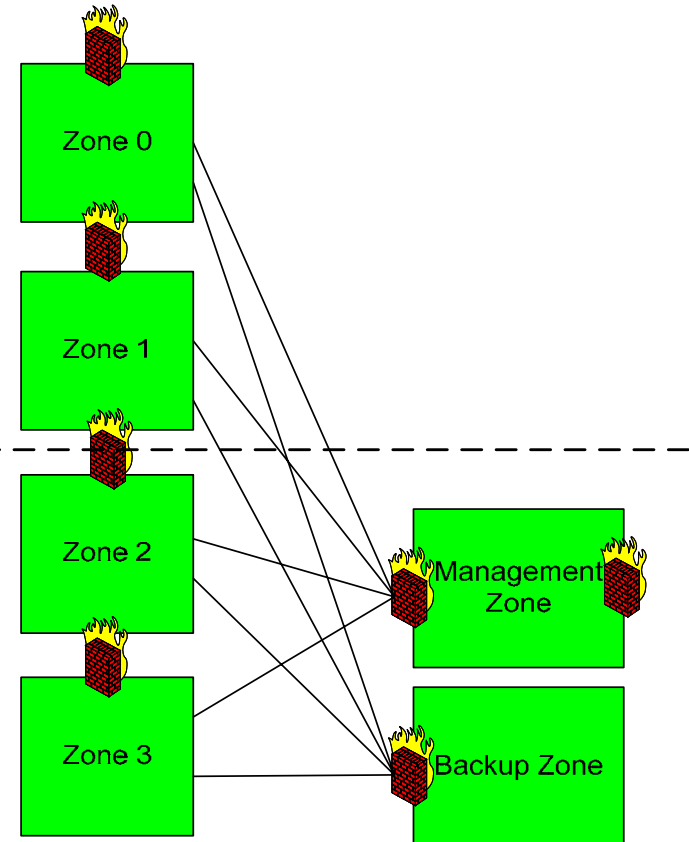


# AHF vs uB1 DMZ

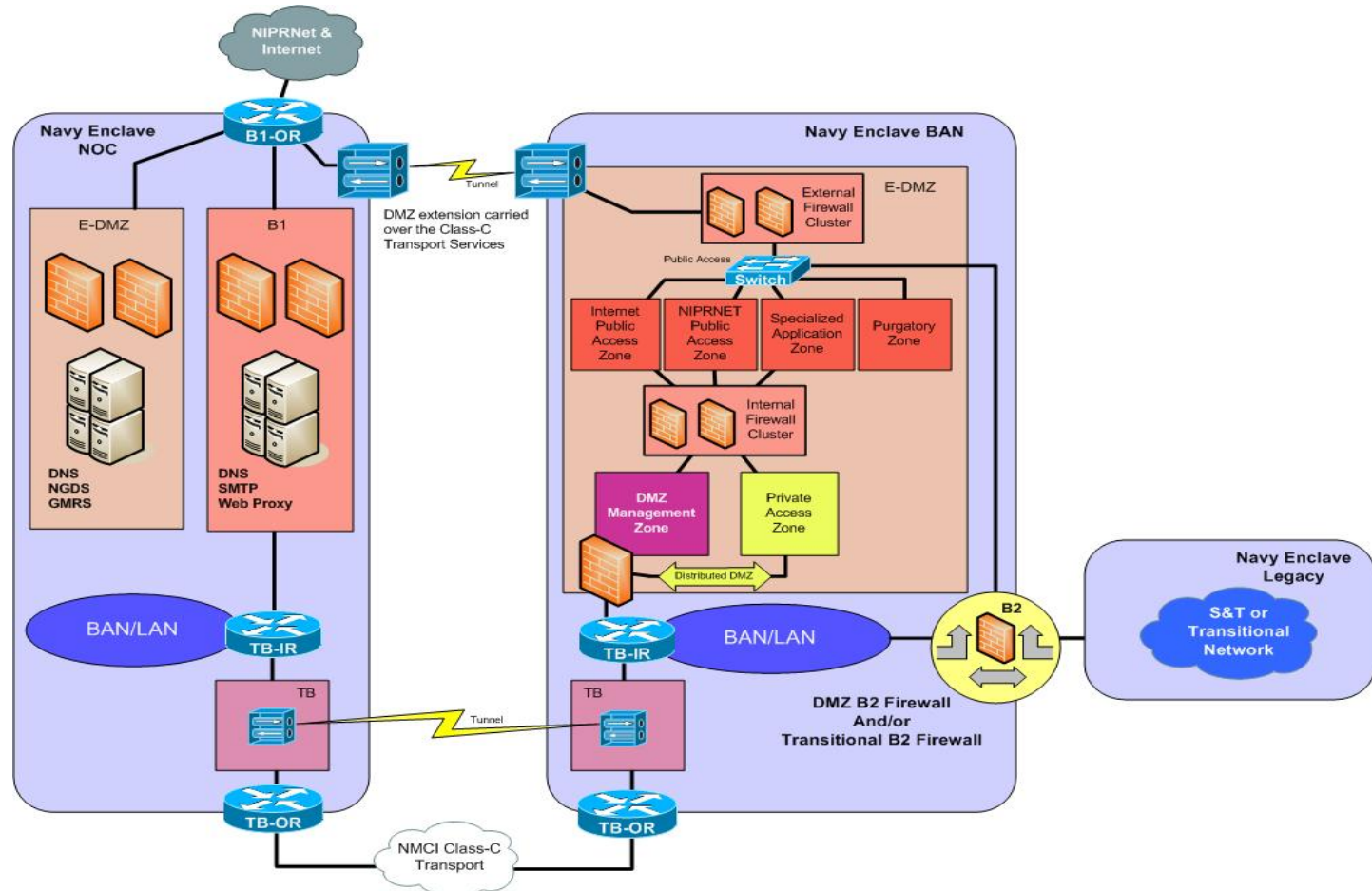
uB1 DMZ



AHF



# DMZ Network Connectivity



## ➤ The uB1 Extension

- ❑ Path utilizes VPN device to securely extend NIPRNet connectivity to Navy-owned server farms
- ❑ Provides a secure extension to remote sites by establishing an encrypted tunnel over NMCI WAN Transport Boundary services between the uB1 and the remote site
- ❑ Each DMZ security zone is capable of being extended to other NMCI sites utilizing the DMZ Extension construct

# Questions?